UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
EASTERN DIVISION

IN RE APPLICATION OF THE UNITED STATES OF AMERICA FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)	**MISC. NO.** 2:19-mj-545 **Filed Under Seal**

APPLICATION OF THE UNITED STATES
FOR AN ORDER PURSUANT TO 18 U.S.C. § 2703(d)

The United States of America, moving by and through its undersigned counsel, respectfully submits under seal this *ex parte* application for an Order pursuant to 18 U.S.C. § 2703(d). The proposed Order would require Microsoft Corporation, an electronic communications service provider and/or a remote computing service, located in Redmond, Washington, to disclose certain records and other information pertaining to the Gmail account **powercyberarmy@outlook.com** as described in Part I of Attachment A. The records and other information to be disclosed are described in Part II of Attachment A to the proposed Order. In support of this application, the United States asserts:

LEGAL BACKGROUND

1. Microsoft Corporation is a provider of an electronic communications service, as defined in 18 U.S.C. § 2510(15), and/or a remote computing service, as defined in 18 U.S.C. § 2711(2). Accordingly, the United States may use a court order issued under § 2703(d) to require Microsoft Corporation to disclose the items described in Part II of Attachment A. *See* 18 U.S.C. § 2703(c)(2) (Part II.A of Attachment A); 18 U.S.C. § 2703(c)(1) (Part II.B of Attachment A).

2. This Court has jurisdiction to issue the proposed Order because it is "a court of competent jurisdiction," as defined in 18 U.S.C. § 2711. *See* 18 U.S.C. § 2703(d). Specifically,

the Court is a district court of the United States that has jurisdiction over the offense being investigated. *See* 18 U.S.C. § 2711(3)(A)(i).

3. A court order under § 2703(d) "shall issue only if the governmental entity offers specific and articulable facts showing that there are reasonable grounds to believe that the contents of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation." 18 U.S.C. § 2703(d). Accordingly, the next section of this application sets forth specific and articulable facts showing that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation.

THE RELEVANT FACTS

4. The United States is investigating unauthorized access in connection with computers. The investigation concerns possible violations of, inter alia, 18 U.S. Code § 1030(a).

5. On or about February 5, 2019, the Indonesian General Elections Commission (KPU)'s website (VICTIM #1) was defaced. A screenshot was uploaded to a KPU webpage. Part of the screenshot contained the words "HACKED BY MR.BINARYCODE", "OPPOSITE6890", and "Moslem Cyber Team". Additionally, a second website was defaced late January or early February 2019. The website, Revolusi Mental (VICTIM #2), contained the exact same screenshot as the VICTIM #1.

6. Open source research of "Mr.Binarycode X" identified an Instagram account mr_binarycode. One of the posts on the account was a picture of a defaced online news website Kabar Indonesia (VICTIM #3). The picture included "Hacked By MR BINARYCODE X OPPOSITE6890 <= MOSLEM CYBER TEAM". At the bottom of the post, an Instagram user

replied that they had opened the website and it was not defaced, to which Target #3 replied that they would hack it again.

7. On April 19, 2019, a 2703(d) Order was served to Instagram for the mr_binarycode account. In the return, **powercyberarmy@outlook.com** was identified as a registered email address.

8. Obtaining records from Microsoft Corporation will help in the identification of the users of the accounts and advance the investigation.

REQUEST FOR ORDER

9. The facts set forth in the previous section show that there are reasonable grounds to believe that the records and other information described in Part II of Attachment A are relevant and material to an ongoing criminal investigation. Specifically, these items will help the United States to identify and locate the individual(s) who are responsible for the events described above, and to determine the nature and scope of their activities. Accordingly, the United States requests that Microsoft Corporation be directed to produce all items described in Part II of Attachment A to the proposed Order.

10. The United States further requests that the Order require Microsoft Corporation not to notify any person, including the subscribers or customers of the account(s) listed in Part I of Attachment A, of the existence of the Order until further order of the Court. *See* 18 U.S.C. § 2705(b). This Court has authority under 18 U.S.C. § 2705(b) to issue "an order commanding a provider of electronic communications service or remote computing service to whom a warrant, subpoena, or court order is directed, for such period as the court deems appropriate, not to notify any other person of the existence of the warrant, subpoena, or court order." *Id.* In this case, such an order would be appropriate because the requested Order relates to an ongoing criminal

investigation that is neither public nor known to all of the targets of the investigation, and its disclosure may alert the targets to the ongoing investigation. Accordingly, there is reason to believe that notification of the existence of the requested Order will seriously jeopardize the investigation, including by giving targets an opportunity to flee or continue flight from prosecution, destroy or tamper with evidence, change patterns of behavior, or notify confederates. *See* 18 U.S.C. § 2705(b)(2), (3), (5). Most, if not all, of the evidence in this investigation is stored electronically. If alerted to the investigation, the subjects under investigation could destroy that evidence, including information saved to their personal computers.

11. The United States further requests that the Court order that this application and any resulting order be sealed until further order of the Court. As explained above, these documents discuss an ongoing criminal investigation that is neither public nor known to all of the targets of the investigation. Accordingly, there is good cause to seal these documents because their premature disclosure may seriously jeopardize that investigation.

Respectfully submitted,

BENJAMIN C. GLASSMAN
United States Attorney

s/ Jessica H. Kim

JESSICA H. KIM (0087831)
Assistant United States Attorney
303 Marconi Boulevard, Suite 200
Columbus, Ohio 43215
Office: (614) 469-5715
Fax: (614) 469-5653
E-mail: Jessica.Kim@usdoj.gov

ATTACHMENT A

I. The Account(s)

The Order applies to certain records and information associated with the following user name(s):

powercyberarmy@outlook.com

II. Records and Other Information to Be Disclosed

Microsoft Corporation is required to disclose the following records and other information, if available, to the United States for each account or identifier listed in Part I of this Attachment ("Account"), for the time periods listed above:

A. The following information about the customers or subscribers of the Account:

1. Names (including subscriber names, user names, and screen names);
2. Addresses (including mailing addresses, residential addresses, business addresses, and e-mail addresses);
3. Local and long distance telephone connection records;
4. Records of session times and durations, and the temporarily assigned network addresses (such as Internet Protocol ("IP") addresses) associated with those sessions;
5. Length of service (including start date) and types of service utilized;
6. Telephone or instrument numbers (including MAC addresses);
7. Other subscriber numbers or identities (including the registration Internet Protocol ("IP") address); and
8. Means and source of payment for such service (including any credit card or bank account number) and billing records.

B. Any and all accounts linked to the listed Account, including other accounts linked by:

1. Creation IP address

2. Creation email address

3. Recovery email address

4. Cookies

5. Telephone number(s) associated with the account

C. Any and all push notification tokens for the listed account and SMS recovery numbers;

D. Any Google Wallet Data to include Google Play service data;

E. A complete listing of all enabled Google Services;

F. Android devices associated with or registered to the account;

G. Any additional user accounts associated with these Android devices;

H. All records and other information (not including the contents of communications) relating to the Account, including:

1. Records of user activity for each connection made to or from the Account, including log files; messaging logs; the date, time, length, and method of connections; data transfer volume; user names; and source and destination Internet Protocol addresses;

2. Information about each communication sent or received by the Account, including the date and time of the communication, the method of communication, and the source and destination of the communication (such as source and destination email addresses, IP addresses, and telephone numbers);

CERTIFICATE OF AUTHENTICITY OF DOMESTIC BUSINESS RECORDS PURSUANT TO FEDERAL RULE OF EVIDENCE 902(11)

I, _____, attest, under penalties of perjury under the laws of the United States of America pursuant to 28 U.S.C. § 1746, that the information contained in this declaration is true and correct. I am employed by Microsoft Corporation, and my official title is _____. I am a custodian of records for Microsoft Corporation I state that each of the records attached hereto is the original record or a true duplicate of the original record in the custody of Microsoft Corporation, and that I am the custodian of the attached records consisting of _____ (pages/CDs/kilobytes). I further state that:

a. all records attached to this certificate were made at or near the time of the occurrence of the matter set forth, by, or from information transmitted by, a person with knowledge of those matters;

b. such records were kept in the ordinary course of a regularly conducted business activity of Microsoft Corporation; and

c. such records were made by Microsoft Corporation as a regular practice.

I further state that this certification is intended to satisfy Rule 902(11) of the Federal Rules of Evidence.

_____ _____

Date Signature